ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Biology, Engineering, Science and Technology (IJARBEST)

Vol. 1, Special Issue 5, May 2013

USB BASED KEYLOCK PROTECTION FOR PRIVACY ENCHANCEMENT

Tinu Mohan

Asst.Professor in Sivaji College of Engineering and Technology
Department of Computer Science
Email id: Tinumohan2014@gmail.com

ABSTRACT

This paper proposes Multifactor authentication schema by combining Token and Graphical password schemas. Token refers to a hardware that is used by each user to prove his/her user identity. To develop a Token based schema IMEI number of the mobile or serial number of the USB devices (storage device) are taken and it is act as the Token for each users. Here serial number or IMEI is unique. Graphical passwords offer an alternative to text-based passwords intended that is to be more memorable and usable because graphical passwords rely on our ability to more accurately remember images than text .Graphical authentication schema proposed here to avoid usability problem of Text-based password schema. By combining Token and Graphical schemas we can avoid the usability problem and ensure towards the user privacy.

Keywords:-Multifactor Authentication, IMEI, USB, Text-based password, Graphical password

I INTRODUCTION

Authentication deals with the security as an act of showing the belongings to its owner only. Various authentication schemes are available these days. But out of these entire how many are truly secure? .To answer it lets go through the background of passwords schema .Authentication is the first step of information security. Authentication schemes require users to memorize the passwords and recall them during log-in time. Current authentication methods can be divided into three main areas: Knowledge based authentication, token based authentication and biometric based authentication.

Knowledge based authentication techniques are most widely used and include text-based and picture-based passwords. Credit card is an example for token based authentication technique. Fingerprints, iris scan, or facial recognition are examples of biometric based authentication. Textual passwords are first choice for authentication by humans. Due to the limitation of human memory, users generally choose the passwords which are easy to remember. The strength of the password depends on size of the memorable password space rather than full password space.

Alphanumerical username/passwords are the most common type of user authentication. They are

versatile and easy to implement and use. Alphanumerical passwords are required to satisfy two contradictory requirements. They have to be easily remembered by a user, while they have to be hard to guess by impostor [2]. Users are known to choose easily guessable and/or short text passwords, which are an easy target of dictionary and brute-forced attacks [3, 4, 5]. Enforcing a strong password policy sometimes leads to an opposite effect, as a user may resort to write his or her difficult to- remember exposing them **Taxonomy of Authentication**

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Biology, Engineering, Science and Technology (IJARBEST)

Vol. 1, Special Issue 5, May 2013

II LITERATURE SURVEY

Knowledge Based Authentication

Knowledge based techniques are the most extensively used authentication techniques and include both text based and picture based passwords.to direct theft.

Most of the authentication system faces security and usability problems. To address this problem token base model is developed. Here the security is in users hand by keeping the token of each user as safe as possible. In addition to the token based schema a graphical schema is introduced to provide a strong multifactor authentication schema that is free from current possible attacks.Knowledge-based authentication (KBA) is based on "Something You Know" to identify you [5] For Example a Personal Identification Number (PIN),password or pass phrase. It is an authentication scheme in which the user is asked to answer at least one "secret" question. KBA is often used as a component in multifactor authentication (MFA) and for self-service password retrieval. Knowledge based authentication (KBA) offers several advantages to traditional (conventional) forms of e-authentication like passwords, PKI and biometrics.

Textual password

In textual passwords, users provide an identifier, a typed in word or phrase. Remembering a p a s s w o r d was relies on p u r e r e c a l l m e m o r y . Textual p a s s w o r d authentication is generally simple and does not require much more processing power.

Graphical Password Systems

Graphical passwords were first described by Blonder [2]. Since then, many other graphical password schemes have been proposed. Graphical password systems can be classified as

- Recognition Based Techniques
- Recall based techniques

Recognition Based Techniques

This graphical authentication scheme is based on the Hash Visualization technique[7]. In this system the user is asked to select a certain number of images from a set of random pictures generated by a program later the user will be required to identify the pre-selected images in order to be authenticated. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Also, the process of selecting a set ofpictures from the picture database can be tedious and time consuming for the user.

Recall based Techniques

In this section there are two recent types of click based graphical password techniques:

1. Cued Click Points (CCP)
2. Persuasive Cued Click- Points (PCCP)

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Biology, Engineering, Science and Technology (IJARBEST)

Vol. 1, Special Issue 5, May 2013

Cued Click Points (CCP)

CCP was developed as an alternative click based graphical password scheme where users select one point per image for five images. The interface displays only one image at a time; the image is replaced by the next image as soon as a user selects a click point. The system determines the next image to display based on the user's click-point on the current image. The next image displayed to users is based on a deterministic function of the point which is currently selected. It now presents a one to-one cued recall scenario where each image triggers the user's memory of the one click-point on that image. Secondly, if a user enters an incorrect click-point during login, the next image displayed will also be incorrect. Legitimate users who see an unrecognized image know that they made an error with their previous click-point. Conversely, this implicit feedback is not helpful to an attacker who does not know the expected sequence of images.

Persuasive Cued Click- Points (PCCP)

To address the issue of hotspots, PCCP was proposed. As with CCP, a password consists of five click points, one on each of five images. During password creation, most of the image is dimmed except for a small view port area that is randomly positioned on the image. Users must select a click-point within the view port. If they are unable or unwilling to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots. A user who is determined to reach a certain click-point may still shuffle until the view port moves to the specific location, but this is a time consuming and more tedious process.

Token Based Authentication:

It is based on "Something You Possess". For example Smart Cards, a driver's license, credit card, a university ID card etc. It allows users to enter their username and password in order to obtain a token which allows them to fetch a specific resource - without using their username and password. Once their token has been obtained, the user can offer the token - which offers access to a specific resource for a time period - to the remote site. Many token based authentication systems also use knowledge based techniques to enhance security.

Biometric Based Authentication:

Biometrics (ancient Greek: bios ="life", metron ="measure") is the study of automated methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. It is based on "Something You Are". It uses physiological or behavioral characteristics like fingerprint or facialscans and iris or voice recognition to identify users. A biometric scanning device takes a user's biometric data, such as an iris pattern or fingerprint scan, and converts it into digital information a computer can interpret and verify.

III USB BASED AUTHENTICATION

In USB based Authentication is based on the lock and key system model. Here each user registers to the system using his/her Mobile IMEI number or serial number of the USB storage device. Serial number or the IMEI number is unique in nature. While the user try login to the system the user identity is only verified by checking the

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Biology, Engineering, Science and Technology (IJARBEST)

Vol. 1, Special Issue 5, May 2013

serial number of the USB device or IMEI of the mobile. After verify the user identity, common procedure is asking for the password. To avoid the memory burden of the existing password schema, graphical authentication is used. Here each user can upload an image and then select 3 spot on the image during the registration time. User must remember the point and the order in which the point is selected. Login time user has to select the selected spot in the correct order for the successful login.

Figure 1. An example of creating a graphical password

In Figure 1, we show an example of a user creating a graphical password. In this example, the user uploads a picture of his or her kids. Then the user clicks on the kids' faces in the order of their ages (order is enforced). Here user has to remember point and the order in which the point is selected.

Since it is almost impossible for human users to click repeatedly on exactly the same point, tolerance region can be found out. It is done find out the distance between the points using distance formula.

$$D = \sqrt{(X_2 - X_1)^2 + (Y_2 - Y_1)^2}$$

D=distance between the points (X1, Y1) is the base co-ordinate (X2, Y2) is the current co-ordinate
If the D is in the acceptable range then password is accept otherwise decline.

Conclusion

User authentication is a fundamental component in most computer security contexts. In this abstract, we proposed a multifactor authentication by combining a token and simple graphical password authentication system. Our preliminary analysis suggests that it is impossible to break USB based Authentication schema using the traditional attack methods such as brute force search, dictionary attack, or spyware.

References

1.Baddeley, A. and Turner, R. spatstat: An R package for Analyzing Spatial Point Patterns. Journal of StatisticalSoftware, v12(6), 2005.

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Biology, Engineering, Science and Technology (IJARBEST)

Vol. 1, Special Issue 5, May 2013

2. Britton, Ian. http://freefoto.com Last accessed Feb.2007.

3. Chiasson, S., Biddle, R., and van Oorschot, P.C. A Second Look at the Usability of Click-Based Graphical Passwords. Symp. on Usable Privacy and Security (SOUPS) 2007.
4. Chiasson, S., van Oorschot, P.C., and Biddle, R. A Usability Study and Critique of Two Password Managers. 15th USENIX Security Symposium, 2006.
5. Chiasson, S., van Oorschot, P.C., Biddle, R. Graphical Password Authentication Using Cued Click-points. ESORICS 2007.
6. Cranor, L.F. and Garfinkel, S. (eds). *Security and Usability: Designing Secure Systems that People Can Use.* O'Reilley Media Inc, Sebastopol, CA, 2005.
7. Davis, D., Monrose, F., Reiter, M.K. On User Choice in Graphical Password Schemes. USENIX Security Symp.2004.
8. Diggle, P.J. *Statistical Analysis of Spatial Point*

Patterns. Academic Press: New York, NY, 1983.

9. Dirik, A.E., Memon, N., and Birget, J.C. Modeling user choice in the PassPoints graphical password scheme. Symp.on Usable Privacy and Security (SOUPS) 2007.
10. Florencio, D. and Herley, C. A Large-scale Study of WWW Password Habits. Proceedings of WWW 2007.